Release Notes for the Cisco ME 3400 Ethernet Access Switch, Cisco IOS Release 12.2(44)SE

January 11, 2008

Cisco IOS Release 12.2(44)SE runs on the Cisco ME 3400 Series Ethernet Access switches.

These release notes include important information about Cisco IOS Release 12.2(44)SE and any limitations, restrictions, and caveats that apply to the release. Verify that these release notes are correct for your switch:

- If you are installing a new switch, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 3.
- If you are upgrading to a new release or different image, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 3.

For the complete list of Cisco ME 3400 switch documentation, see the "Related Documentation" section on page 25.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Contents

This information is in the release notes:

- "Hardware Supported" section on page 2
- "Upgrading the Switch Software" section on page 2
- "Installation Notes" section on page 5

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

- "New Features" section on page 5
- "Minimum Cisco IOS Release for Major Features" section on page 6
- "Limitations and Restrictions" section on page 8
- "Open Caveats" section on page 13
- "Resolved Caveats" section on page 15
- "Documentation Updates" section on page 18
- "Related Documentation" section on page 25
- "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page 25

Hardware Supported

Table 1 lists the hardware supported on Cisco IOS Release 12.2(44)SE.

Table 1 Supported Hardware

Device	Description	Supported by Minimum Cisco IOS Release
ME 3400-24FS-A	24 100BASE-FX SFP module ports and 2 Gigabit Ethernet SFP module ports, AC power	Cisco IOS Release 12.2(40)SE
ME 3400G-2CS	2 dual-purpose ports and 2 SFP-only module ports, AC power	Cisco IOS Release 12.2(35)SE1
ME-3400G-12CS-A	12 dual-purpose ports and 4 SFP-only module ports	Cisco IOS Release 12.2(25)SEG1
ME-3400G-12CS-D	12 dual-purpose ports and 4 SFP-only module ports	Cisco IOS Release 12.2(25)SEG1
ME-3400-24TS-A	24 10/100 ports and 2 SFP module slots, AC power	Cisco IOS Release 12.2(25)EX
ME-3400-24TS-D	24 10/100 ports and 2 SFP module slots, DC power	Cisco IOS Release 12.2(25)EX
SFP modules	1000BASE-T, -BX, -SX, -LX/LH, -ZX 100BASE-BX, FX, -LX Coarse wavelength-division multiplexing (CWDM)	Cisco IOS Release 12.2(25)EX
Cable	Catalyst 3560 SFP interconnect cable	Cisco IOS Release 12.2(25)EX

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

- "Finding the Software Version and Feature Set" section on page 3
- "Deciding Which Files to Use" section on page 3
- "Archiving Software Images" section on page 3
- "Upgrading a Switch" section on page 4
- "Recovering from a Software Failure" section on page 5

Finding the Software Version and Feature Set

The Cisco IOS image is stored as a bin file in a directory that is named with the Cisco IOS release. The image is stored on the system board flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line of the display shows the version.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Deciding Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined tar file. This file contains the Cisco IOS image file. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 2 lists the filenames for this software release.

Table 2 Cisco IOS Software Image Files

Filename	Description
me340x-metrobase-tar.122-44.SE.tar	Cisco ME 3400 metro base image. This image has basic Metro Ethernet features.
me340x-metrobasek9-tar.122-44.SE.tar	Cisco ME 3400 metro base cryptographic image. This image has the Kerberos, Secure Shell (SSH), and basic Metro Ethernet features.
me340x-metroaccess-tar.122-44.SE.tar	Cisco ME 3400 metro access image. This image has Layer 2 + Metro Ethernet features.
me340x-metroaccessk9-tar.122-44.SE.tar	Cisco ME 3400 metro access cryptographic image. This image has the Kerberos, SSH, and Layer 2 + Metro Ethernet features.
me340x-metroipaccess-tar.122-44.SE.tar	Cisco ME 3400 metro IP access image. This image has Layer 2+ and full Layer 3 routing Metro Ethernet features.
me340x-metroipaccess9-tar.122-44.SE.tar	Cisco ME 3400 metro IP access cryptographic image. This image has the Kerberos, SSH, Layer 2+, and full Layer 3 routing Metro Ethernet features.

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release to which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca744.html#wp1018426

Upgrading a Switch

This procedure is for copying the combined tar file to the switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

Note For downloading software, we recommend that you connect to the TFTP server through a network node interface (NNI). If you want to connect to the server through a user network interface (UNI), see the "Troubleshooting" chapter of the software configuration guide for methods for enabling ping capability on UNIs. See the "New Software Features" section on page 6 for a definition of NNIs and UNIs.

To download software, follow these steps:

Step 1 Use Table 2 on page 3 to identify the file that you want to download.

Step 2 Download the software image file. If you have a SmartNet support contract, log in to cisco.com and go to this URL, and log in to download the appropriate files:

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

Click on "*Launch the IOS Upgrade Planner*" and search for ME 3400 to download the appropriate files:

- To download the metro base, metro access, or metro IP access files for a Cisco ME 3400 switch, click **Cisco ME 3400 software**.
- To obtain authorization and to download the cryptographic software files, click **Cisco ME 3400 3DES Cryptographic Software**.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

Note By default, ping is supported on network node interfaces (NNIs), but you cannot ping from a user network interface (UNI) because the control-plane security feature drops ICMP response packets received on UNIs. See the "Troubleshooting" chapter of the software configuration guide for methods for pinging from the switch to a host connected to a UNI.

For more information about assigning an IP address and default gateway to the switch, refer to the software configuration guide for this release.

Step 6 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by entering this privileged EXEC command:

```
Switch# archive download-sw /overwrite /reload
tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved.

For *//location*, specify the IP address of the TFTP server.

For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite
tftp://198.30.20.19/me340x-metroipaccess-tar.122.44.SE.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

For recovery procedures, see the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Features

These sections describe the new supported hardware and the new software features provided in this release:

- “New Hardware Features” section on page 6
- “New Software Features” section on page 6

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

These are the new software features for Cisco IOS Release 12.2(44)SE:

- DHCP-based autoconfiguration and image update to download a specified configuration and image to a large number of switches
- Configurable small-frame arrival threshold to prevent storm control when small frames (64 bytes or less) arrive on an interface at a specified rate (the threshold)
- Source Specific Multicast (SSM) mapping for multicast applications to provide a mapping of source to allowing IGMPv2 clients to utilize SSM, allowing listeners to connect to multicast sources dynamically and reducing dependencies on the application
- Support for the *, *ip-address*, **interface** *interface-id*, and **vlan** *vlan-id* keywords with the **clear ip dhcp snooping** command
- Flex Link Multicast Fast Convergence, which reduces the multicast traffic convergence time after a Flex Link failure
- IEEE 802.1x readiness check to determine the readiness of connected end hosts before configuring IEEE 802.1x on the switch
- Configurable control-plane queue assignment to assign control plane traffic for CPU-generated traffic to a specific egress queue
- Configurable control plane security that provides service providers with the flexibility to drop customers control-plane traffic on a per-port, per-protocol basis. Allows configuring of enhanced network interfaces (ENIs), customer-facing ports that support protocol control packets

Minimum Cisco IOS Release for Major Features

Table 3 lists the minimum software release (after the first release) required to support the major features of the Cisco ME 3400 switch. Features not listed are supported in all releases.

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required

Feature	Minimum Cisco IOS Release Required
DHCP-based autoconfiguration and image update	12.2(44)SE
Configurable small-frame arrival threshold	12.2(44)SE
Source Specific Multicast (SSM) mapping for multicast applications	12.2(44)SE
Support for the *, *ip-address*, **interface** *interface-id*, and **vlan** *vlan-id* keywords with the **clear ip dhcp snooping** command	12.2(44)SE
Flex Link Multicast Fast Convergence	12.2(44)SE
IEEE 802.1x readiness check	12.2(44)SE
Configurable control-plane queue assignment	12.2(44)SE

Table 3 Features Introduced After the First Release and the Minimum Cisco IOS Release Required (continued)

Feature	Minimum Cisco IOS Release Required
Configurable control plane security (support for ENIs)	12.2(44)SE
Configuration rollback and replacement	12.2(40)SE
EEM (metro IP access image only) **Note** EEM support was added to the metro IP access image in 12.2(44)SE	12.2(40)SE
IGMP Helper (metro IP access image only)	12.2(40)SE
IP SLAs support (metro IP access and metro access images only)	12.2(40)SE
IP SLAs enhanced object tracking (metro IP access and metro access images only)	12.2(40)SE
IP SLAs for Ethernet OAM (metro IP access image only)	12.2(40)SE
Multicast VRF Lite (metro IP access image only)	12.2(40)SE
SSM PIM (metro IP access image only)	12.2(40)SE
REP (metro IP access and metro access images only)	12.2(40)SE
LLDP-MED location TLV (metro IP access and metro access images only)	12.2(40)SE
ELMI-CE	12.2(37)SE
LLDP and LLDP-MED	12.2(37)SE
Port security on a PVLAN host	12.2(37)SE
VLAN Flex Links load balancing	12.2(37)SE
Support for Multicast VLAN Registration (MVR) over trunk ports	12.2(35)SE1
Enhanced object tracking for HSRP (metro IP access image only)	12.2(35)SE1
Ethernet OAM IEEE 802.3ah protocol (metro IP access and metro access images only)	12.2(35)SE1
Ethernet OAM CFM (IEEE 802.1ag) and E-LMI (metro IP access and metro access images only)	12.2(25)SEG
Per port per VLAN QoS (metro IP access and metro access images only)	12.2(25)SEG
Support for all OSPF network types (metro IP access only)	12.2(25)SEG
Layer 2 protocol tunneling on trunks (metro IP access and metro access images only)	12.2(25)SEG
IS-IS protocol (metro IP access only)	12.2(25)SEG
NNIs on all ports (metro IP access image only)	12.2(25)SEG
DHCP server	12.2(25)SEG
DHCP Option-82 configurable remote ID and circuit ID	12.2(25)SEG
Multiple spanning-tree (MST) based on the IEEE 802.1s standard	12.2(25)SEG
Nonstop forwarding (NSF) awareness (metro IP access image only)	12.2(25)SEG
Secure Copy Protocol	12.2(25)SEG
Flex Links sub 100 ms convergence; preemptive switchover (metro IP access and metro access images)	12.2(25)SEG
Link-state tracking (trunk failover) (metro IP access and metro access images only)	12.2(25)SEG

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

These limitations apply to the Cisco ME switches:

- "Configuration" section on page 8
- "EtherChannel" section on page 9
- "IP" section on page 10
- "MAC Addressing" section on page 10
- "Multicasting" section on page 10
- "Routing" section on page 11
- "QoS" section on page 11
- "SPAN and RSPAN" section on page 12
- "Trunking" section on page 12
- "VLAN" section on page 13

Configuration

These are the configuration limitations:

- When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

  High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

  Use one of these workarounds:

  - Disable logging to the console.
  - Rate-limit logging messages to the console.
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted without a configuration (no config.text file in flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- The DHCP snooping binding database is not written to flash memory or a remote file in any of these situations:
  - When the Network Time Protocol (NTP) is configured, but the NTP clock is not synchronized. You can check the clock status by entering the **show NTP status** privileged EXEC command and verifying that the network connection to the NTP server and the peer work correctly.
  - The DHCP snooping database file is manually removed from the file system. After enabling the DHCP snooping database by configuring a database URL, a database file is created. If the file is manually removed from the file system, the DHCP snooping database does not create another database file. You need to disable the DHCP snooping database and enable it again to create the database file.
  - The URL for the configured DHCP snooping database was replaced because the original URL was not accessible. The new URL might not take effect after the timeout of the old URL.

  No workaround is necessary; these are the designed behaviors. (CSCed50819)
- When dynamic ARP inspection is enabled on a switch, ARP and RARP packets greater than 2016 bytes are dropped by the switch or switch stack. This is a hardware limitation.

  However, when dynamic ARP inspection is not enabled and a jumbo MTU is configured, ARP and RARP packets are correctly bridged in hardware. (CSCed79734)
- Dynamic ARP inspection log entries might be lost after a switch failure. Any log entries that are still in the log buffer (have not been output as a system message) on a switch that fails are lost.

  When you enter the **show ip arp inspection log** privileged EXEC command, the log entries from all switches in the stack are moved to the switch on which you entered the command.

  There is no workaround. (CSCed95822)
- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)
- A traceback error occurs if a crypto key is generated after an SSL client session.

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

EtherChannel

This is the EtherChannel limitation:

- The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

  ```
  15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
  (ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
  4CEB50 859DF4 A7BF28 A98260 882658 879A58
  ```

  There is no workaround. (CSCsh12472)

IP

These are the IP limitations:

- Subnetwork Access Protocol (SNAP) encapsulated IP packets are dropped without an error message being reported at the interface. The switch does not support SNAP-encapsulated IP packets. There is no workaround. (CSCdz89142)
- The switch does not create an adjacent table entry when the ARP timeout value is 15 seconds and the ARP request times out. The workaround is to not set an ARP timeout value lower than 120 seconds. (CSCea21674)

MAC Addressing

This is the MAC addressing limitation:

When a MAC address is configured for filtering on the internal VLAN of a routed port, incoming packets from the MAC address to the routed port are not dropped. (CSCeb67937)

Multicasting

These are the multicasting limitations:

- The switch does not support tunnel interfaces, including DVMRP and PIM tunneling.
- Nonreverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in another VLAN. Because unnecessary traffic is sent on the trunk port, it reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member of the group in at least one VLAN, this problem occurs for the non-RPF traffic. (CSCdu25219)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- When you use the **ip access-group** interface configuration command with a router access control list (ACL) to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN, regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)

- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)
- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

  The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

  There is no workaround. (CSCee16865)
- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

Routing

These are the routing limitations:

- The switch does not support tunnel interfaces for routed traffic.
- A route map that has an ACL with a Differentiated Services Code Point (DSCP) clause cannot be applied to a Layer 3 interface. The switch rejects this configuration and displays a message that the route map is unsupported. There is no workaround. (CSCea52915)
- A spanning-tree loop might occur if all of these conditions are true:
  - Port security is enabled with the violation mode set to protected.
  - The maximum number of secure addresses is less than the number of switches connected to the port.
  - There is a physical loop in the network through a switch whose MAC address has not been secured, and its BPDUs cause a secure violation.

  The workaround is to change any one of the listed conditions. (CSCed53633)

QoS

These are the quality of service (QoS) limitations:

- When you use the **bandwidth** policy-map class command to configure more than one class in a policy map for Class-based Weighted Fair Queuing (CBWFQ), and the committed information rate (CIR) bandwidth for any of the classes is less than 2 percent of the interface rate, the CBWFQ classes in the policy may not receive the configured CIR bandwidths.

  There is no workaround, but it is unlikely that a CBWFQ class would be configured with such a low CIR bandwidth. (CSCsb98219)

- Although visible in the command-line help, the **conform-action color** policy-map class police configuration command is not supported. Entering the command has no affect.

  There is no workaround. (CSCsk00594)

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- The egress SPAN data rate might degrade when multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN at up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If multicast routing is disabled, egress SPAN is not degraded.

  There is no workaround. If possible, disable multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)

- Some IGMP report and query packets with IP options might not be ingress-spanned. Packets that are susceptible to this problem are IGMP packets containing 4 bytes of IP options (IP header length of 24). An example of such packets would be IGMP reports and queries having the router alert IP option. Ingress-spanning of such packets is not accurate and can vary with the traffic rate. Typically, very few or none of these packets are spanned. There is no workaround. (CSCeb23352)

- When system jumbo MTU size is configured on a switch and the egress ports can support jumbo frames, the egress SPAN jumbo frames are not forwarded to the SPAN destination ports.

  There is no workaround. (CSCsj21718)

- Cisco Discovery Protocol (CDP) and Port Aggregation Protocol (PAgP) packets received by network node interfaces (NNIs) from a SPAN source are not sent to the destination interfaces of a local SPAN session.

  The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking

These are the trunking limitations:

- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y, even though the port has no group membership in VLAN Y. There is no workaround. (CSCdz42909).

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics. There is no workaround. (CSCec35100).

VLAN

These are the VLAN limitations:

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to not configure more than the recommended number of VLANs and trunks. (CSCeb31087)

- A CPUHOG message sometimes appears when you configure a private VLAN. Enable port security on one or more of the ports affected by the private VLAN configuration.

  There is no workaround. (CSCed71422)

Open Caveats

This section describes the open caveats in this software release.

- CSCse11323

  When 256 policy maps are configured globally on the system, the creation of the 257th policy map is rejected. The platform supports a maximum of 256 policy maps. If you then delete some existing policy maps and again configure the rejected policy map, when you try to attach that policy map to an interface, it might be rejected without any descriptive error message explaining the reason for the rejection or with an unexpected and incorrect error message.

  The workaround is to delete the problematic policy map and to reconfigure it with a different name. The new policy map should be accepted as expected.

- CSCsi01526

  Traceback messages appear if you enter the **no switchport** interface configuration command to change a Layer 2 interface that belongs to a port channel to a routed port.

  There is no workaround.

- CSCsi06399

  When a RIP network and IP address are configured on an interface, a traceback error occurs after you enter the **shutdown**, **no shutdown, switchport** and **no switchport** interface configuration commands.

  The workaround is to configure the RIP network and the IP address after you configure the interface.

- CSCsi06578

  When you clear counters on an interface and then disable storm control on that interface, an incorrect value (an unusually large number) for McastSuppDiscards appears when you enter the **show interface counters** privileged EXEC command. This can occur when the interface had storm control enabled and experienced traffic with a data rate higher than the storm-control threshold so that storm control is dropping packets.

  There is no workaround.

- CSCsk53850

  If you enter the **no ip vrf** *vrf-name* global configuration command to delete a VPN routing/forwarding instance on the switch when routing is not enabled on the switch, the VRF instance is held in the delete queue. The VRF entry does not appear in the output when you enter the **show running-config** privileged EXEC command, but it is shown when you enter the **show ip vrf** privileged EXEC command. When a VRF instance is in the deleted queue, it is using one of the system's maximum allowable VRFs, and you cannot configure a new VRF with the same name.

  The workaround is to enable IP routing on the switch by entering the **ip routing** global configuration. When you enable routing, the VRF is cleared from the deleted queue.

- CSCsk58435

  When several per-port, per-VLAN parent policies are attached to the input of one or more interfaces and a child policy of these parent policies is modified, the parent policies are detached from the interfaces and reattached during the process. Because the modified policy is large, the TCAM entries are being used up, and the attached policies should be removed. However, some of the parent policies are not removed from the interface, and the TCAM entries are cleared. If you save the configuration and reload the switch, the policies are detached, but the TCAM is full, and you cannot attach other policies.

  This error message appears:

  ```
  QOSMGR-4-QOS_TCAM_RESOURCE_EXCEED_MAX: Exceeded a maximum of QoS TCAM resources
  ```

  The workaround is to manually detach the policy maps from all the interfaces by entering the **no service-policy input** *policy-map-name* interface configuration command on each interface.

- CSCsk65142

  When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command.

- CSCsl46356

  The switch might reload with no stack trace information if you try to configure REP when there a large number of MAC addresses (more than 8000) on more than 900 VLANs on the switch.

  The workaround is to allow a smaller set of MAC addresses (6500) when you configure REP on the switch.

- CSCsm08603

  This traceback error appears when you enter the **show aaa subscriber** *profile* privileged EXEC command:

  ```
  *Mar 2 01:50:41.127: %PARSER-3-BADSUBCMD: Unrecognized subcommand 10 in exec command
  'show aaa subscriber profile WORD'
  -Traceback= D003B4 D00AC8 C908A0 C2F040 C8CA18 CB8984 93B670 932338
  ```

  There is no workaround. This does not affect switch functionality.

Resolved Caveats

These caveats have been resolved in this release:

- CSCsd01180

  The switch no longer reloads when you use a Kron command scheduler routine to automatically copy configuration data using the Secure Copy Protocol (SCP). (Kron is a Cisco IOS utility for scheduling non-prompting CLI commands to execute at a later time.)

- CSCse07183

  While attaching a Per-Port Per Vlan (PPPV) policy-map to an interface, the attachment fails if this policy-map has classes with configured overlapping VLANs. In previous releases, this condition did not exist.

- CSCse14774

  When a switch is connected to a third-party router through an EtherChannel and the EtherChannel is running in Link Aggregation Control Protocol (LACP) mode, the interfaces in the EtherChannel no longer fail after you enter the **switchport trunk native vlan vlan-id** interface configuration command to change the native VLAN from VLAN 1 (the default) to a different VLAN ID.

- CSCse33881

  The switch no longer reloads if you attach an input per-port, per-VLAN hierarchical policy map to a port when the total number of active VLANs being classified in the policy exceeds 255.

- CSCse85482

  If the duplex mode of a GLC-T SFP module that is installed in a Cisco ME-3400G-12CS or ME-3400 2CS switch dual media port is changed from full to half (or the reverse), the mode change immediately reflects in the hardware, and the link operates with the changed setting.

- CSCsg70630

  A switch with the Dynamic ARP Inspection feature enabled no longer experiences the issue that triggered the display of *buffer sharecount* messages under certain patterns of ARP packet traffic.

- CSCsh74395

  When a VLAN includes multiple MAC addresses, the number of MAC addresses shown in SNMP now matches the output of the **show mac-address count vlan** *vlan-id* privileged EXEC command.

- CSCsi06228

  The switch no longer allows an attached policy-map with a **match cos class-map** statement to an IEEE 802.1Q tunnel port. (A **match cos class-map** configuration is only supported on IEEE 802.1Q trunk ports and should be blocked on IEEE 802.1Q tunnel ports.)

- CSCsi63999

  Changing the spanning tree mode from MSTP to other spanning modes no longer causes tracebacks.

- CSCsi67680

  When the switch has VRF interfaces configured and you disable unicast routing by entering the **no ip routing** global configuration command and then re-enable unicast routing, VRF routing now functions correctly over the VRF interface.

- CSCsi77705

  Broadcast storm control now works correctly on IEEE 802.1Q trunk ports.

- CSCsi78737

  The cpmCPURisingThreshold traps on the switch are no longer missing the cpmProcExtUtil5SecRev and cpmProcessTimeCreated trap components. Note that although the components were missing from the traps, the PROCESS MIB was still populating the objects.

- CSCsi79504

  OSPF hello packets now have the correct CoS value of 7.

- CSCsi85257

  A Cisco IP Phone now works correctly when it is connected to a port that is configured with CDP bypass and multidomain authentication (MDA).

- CSCsj22994

  ACLs are now configured correctly when they contain ICMP codes 251 to 255.

- CSCsj47067

  If you upgrade from Cisco IOS Release 12.2(35)SE1 to Release 12.2(37)SE, a security violation no longer occurs when:

  – You enter the **switchport port-security maximum 1 vlan access** interface configuration command.

  – An IP phone with a PC behind it is connected to an access port with port security.

- CSCsj53001

  The Total- output-drops field in the **show interfaces** privileged EXEC command output now displays accurate ASIC drops.

- CSCsj64882

  When IGMP snooping is enabled, CGMP interoperability mode now works as it should when the upstream multicast router is set up correctly with PIM and IP CGMP.

- CSCsj77933

  If you enter a space before a comma in the **define interface-range** or the **interface range** global configuration command, the space before the comma is now saved in the switch configuration.

- CSCsj87991

  A switch configured for Link Layer Discovery Protocol (LLDP) now correctly reports the enabled switch capabilities in the LLDP type, length, and value (TLV) attributes.

- CSCsk34118

  On a switch with routed ports, when you configure MAC address-table aging time by entering the **mac address-table aging-time** *time* global configuration command and then enter the **show running-config** privileged EXEC command, the output no longer displays the aging time values for internal VLANs.

- CSCsk38083

  When UDLD is enabled on a Layer 2 interface, and the native VLAN for the port is not configured as a VLAN on the switch, UDLD no longer puts the port into an error-disabled state.

- CSCsk59299

  When an egress port shaper policy is configured, the switch now correctly polices the traffic down to the right bandwidth instead of to the next lower available rate.

- CSCsk61854

  When two metro Ethernet switches are indirectly connected and the link status of two interfaces that have Resilient Ethernet Protocol (REP) enabled goes down, when one of the links recovers, the port status now correctly changes to open, and traffic resumes through the ring topology.

- CSCsk62010

  A switch no longer fails when you enter the **show interfaces vlan** *vlan-id* **switchport** privileged EXEC command.

- CSCsk67358

  When REP is enabled on the switch, you no longer experience a long recovery time after you disconnect the power cord or shut down a port that has an alternate peer port blocking all VLANs.

- CSCsk67520

  If you enter the **hostname** global configuration command followed by a hostname that contains illegal characters, for example, one that appears to be an IP address, the switch now displays a warning message, but the specified hostname is configured.

- CSCsk75111

  When you configure QoS on the switch, the switch no longer reloads if you detach a service policy from an interface and then enter a qualified queue-limit command in a policy map and attach the policy map to the interface.

- CSCsk84233

  A switch no longer fails under these conditions:

  – EIGRP routing is enabled.

  – The HSRP standby interface and the active interface are configured with the same IP address.

  – A switch that is connected to the HSRP standby interface fails.

- CSCsk93195

  The ME 3400 switch now supports EEM in the metro access image.

- CSCsl09845

  A switch no longer unexpectedly reloads when you delete a VLAN interface that is configured with a (user-network interface) UNI.

- CSCsl31389

  Flex Link backup ports now correctly block IEEE 802.1ag Connectivity Fault Management (CFM) frames.

- CSCsl33304

  Web authentication no longer stops working when IEEE 802.1X re-authentication is enabled and the re-authentication timer expires.

Documentation Updates

This section contains these documentation updates:

- "Updates to the Software Configuration Guide" section on page 18
- "Updates to the Command Reference" section on page 19
- "Updates to the System Message Guide" section on page 20
- "Update to the Regulatory Compliance and Safety Information" section on page 22
- "Updates to the Hardware Installation Guide" section on page 23

Updates to the Software Configuration Guide

These are the updates to the software configuration guide:

- This information in the "Enabling BPDU Guard" section of the "Configuring Optional Spanning-Tree Features" chapter in the software configuration guide is incorrect:

  When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree shuts down Port Fast-enabled ports that receive BPDUs.

  This is the correct information:

  When you globally enable BPDU guard on ports that are Port Fast-enabled (the ports are in a Port Fast-operational state), spanning tree continues to run on the ports. They remain up unless they receive a BPDU.

- In the "Multi-VRF CE Configuration Guidelines" section of the "Configuring IP Unicast Routing" chapter of the *Cisco ME 3400 Switch Software Configuration Guide*, this guideline is incorrect:

  If no VRFs are configured, 104 policies can be configured.

  This is the correct guideline:

  If no VRFs are configured, up to 105 policies can be configured.

- In the "Configuring Resilient Ethernet Protocol" chapter in the software configuration guide, and in the command reference, the allowed range for the r**ep admin vlan** *vlan-id* global configuration command is shown as 1 to 4094. The correct range is 2 to 4094. To set the admin VLAN to 1, enter the **no rep admin vlan** global configuration command to return it to the default.

- This information is added to the "Using IEEE 802.1x Authentication with Per-User ACLs" section of "Configuring IEEE 802.1x Port-Based Authentication" chapter of the software configuration guide:

  Per-user ACLs are supported only in single-host mode.

Updates to the Command Reference

These are updates to the command reference:

- Although visible in the command-line help, the **conform-action color** policy-map class police configuration command is not supported. Entering the command has no affect.
- The usage guidelines for the **set** and **unset** bootloader commands in the command reference are incorrect.

  These are the correct usage guidelines for the **set** command:

  Environment variables are case sensitive and must be entered as documented.

  Environment variables that have values are stored in flash memory outside of the flash file system.

  Under normal circumstances, it is not necessary to alter the setting of the environment variables.

  The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

  The BOOT environment variable can also be set by using the **boot system** *filesystem***:/***file-url* global configuration command.

  The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

  The HELPER environment variable can also be set by using the **boot helper** *filesystem***:/***file-url* global configuration command.

  The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:/***file-url* global configuration command.

  The HELPER_CONFIG_FILE environment variable can also be set by using the **boot helper-config-file** *filesystem***:/***file-url* global configuration command.

  The bootloader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

  These are the correct guidelines for the **unset** command:

  Under normal circumstances, it is not necessary to alter the setting of the environment variables.

  The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

  The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

  The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

  The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

  The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

  The HELPER_CONFIG_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command.

Updates to the System Message Guide

These sections include messages that have been added to or changed in the system message guide.

New System Messages

These new messages have been added to the system message guide:

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars]`

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. [enet] is the supplicant MAC address, and [chars] is the interface. This message might appear if the IEEE 802.1x feature is enabled.

Recommended Action If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, manually remove it from that port.

Error Message `SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans`

Explanation The interface has been added to all VLANs. [chars] is the added interface.

Recommended Action No action is required.

Error Message `SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans`

Explanation The interface has been deleted from all VLANs. [chars] is the deleted interface.

Recommended Action No action is required.

Error Message `SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].`

Explanation The VLAN Trunking Protocol (VTP) domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

Recommended Action No action is required.

Error Message `PLATFORM_ENV-1-DUAL_PWR: Faulty internal power supply [chars] detected`

Explanation A faulty internal power supply was detected in one of the two power supplies on the switch. [chars] is the power supply name.

Recommended Action Copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the error by using the Output Interpreter. Use the Bug Toolkit to look for similar reported problems. If you still require assistance, open a case with the TAC, or contact your Cisco technical support representative, and provide the representative with the gathered information. For more information about these online tools and about contacting Cisco, see the “Error Message Tracebacks Reports” section of the system message guide.

Error Message `PLATFORM_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix`

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ip unicast failed route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message `REP-4-LINKSTATUS: [chars] (segment [dec]) is [chars]`

Explanation The Resilient Ethernet Protocol (REP) link status has changed. The first [chars] is the interface name that has a link-status change. The [dec] is the REP segment number of the interface. The second [chars] is the new link status.

Recommended Action No action is required.

Error Message `REP-5-PREEMPTIONFAIL: can not perform preemption on segment [dec] due to [char]`

Explanation The Resilient Ethernet Protocol (REP) preempt operation failed. This could be due to an invalid port ID or a neighbor_offset number specified with the **rep block port** interface configuration command. This could also be caused by entering the **rep block port preferred** interface configuration command if there is no REP port configured with the **preferred** keyword. [dec] is the segment number, and [char] is the reason for the failure.

Recommended Action Correct the configuration, and run REP manual preemption on the primary edge port by entering the **rep preempt segment** command.

Changed System Message

This system message has changed (both explanation and action).

Error Message `EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.`

Explanation The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel. The second [chars] is the port number.

Recommended Action Ensure that the other ports in the bundle have the same configuration.

Update to the Regulatory Compliance and Safety Information

The Regulatory Compliance Standards section of the *Regulatory Compliance and Safety Information for the Cisco ME 3400 and Cisco ME 2400 Ethernet Access Switches* includes this new section:

Cautions and Regulatory Compliance Statements for NEBS

This section includes the cautions and regulatory compliance statements for the Network Equipment-Building System (NEBS) certification from the *Telcordia Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment* (A Module of LSSGR, FR-64; TSGR, FR-440; and NEBSFR, FR-2063) Telcordia Technologies Generic Requirements, GR-1089-CORE, Issue 4, June 2006.

Table 4 NEBS Compliance Statements

Attach an ESD-preventive wrist strap to your wrist and to a bare metal surface.
Caution To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, for Ethernet RJ-45 ports, use only shielded Ethernet cables that are grounded on both ends. In a NEBS installation, all Ethernet ports are limited to intrabuilding wiring.
Caution The intrabuilding ports of the equipment or subassembly is only suitable for connection to intrabuilding or unexposed wiring or cabling. The intrabuilding ports of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use only as intrabuilding interfaces (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4), and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection in order to connect these interfaces metallically to OSP wiring.
Products that have an AC power connection are intended for deployments where an external surge protective device (SPD) is used at the AC power service equipment as defined by the National Electric Code (NEC).
This product is designed for a common bonding network (CBN) installation.
This product can be installed in a network telecommunication facility or location where the NEC applies.
An electrical conducting path should exist between the product chassis and the metal surface of the enclosure or rack in which it is mounted or to a grounding conductor. Electrical continuity should be provided by using thread-forming type mounting screws that remove any paint or nonconductive coatings and establish a metal-to-metal contact. Any paint or other nonconductive coatings should be removed on the surfaces between the mounting hardware and the enclosure or rack. The surfaces should be cleaned and an antioxidant applied before installation.

Table 4 NEBS Compliance Statements (continued)

The grounding architecture of this product is DC-isolated (DC-I).
DC-powered products have a nominal operating DC voltage of 48 VDC. Minimal steady state DC operating voltage is 40 VDC. Reference American National Standards Institute (ANSI) T1.315, Table 1.

Updates to the Hardware Installation Guide

These are updates to the *Cisco ME 3400 Hardware Installation Guide*:

- "Installation Information" section on page 23
- "Update to Appendix C" section on page 23

Installation Information

Cisco Ethernet Switches are equipped with cooling mechanisms, such as fans and blowers. However, these fans and blowers can draw dust and other particles, causing contaminant buildup inside the chassis, which can result in a system malfunction.

You must install this equipment in an environment as free as possible from dust and foreign conductive material (such as metal flakes from construction activities).

These standard provide guidelines for acceptable working environments and acceptable levels of suspended particulate matter:

- Network Equipment Building Systems (NEBS) GR-63-CORE
- National Electrical Manufacturers Association (NEMA) Type 1
- International Electrotechnical Commission (IEC) IP-20

Update to Appendix C

This information is being added to the "Wiring the DC-Input Power Source" section of Appendix C, "Connecting to DC Power," in the *Cisco ME 3400 Ethernet Access Switch Hardware Installation Guide*:

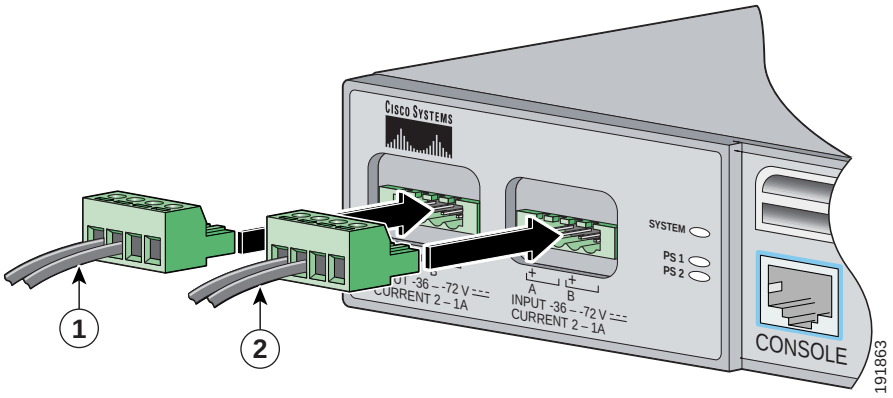
Before you wire the DC-input power source, review the warnings in this section and this information:

If the switch software detects that the circuit boards are not receiving power from an internal power supply, the software sends a message like this to the console:

```
00:06:54: %POWER_SUPPLIES-3-PWR_FAIL: Power supply 2 is not functioning
00:06:54: %PLATFORM_ENV-1-DUAL_PWR: Faulty internal power supply 2 detected
```

This message means that an internal power supply is not providing power. To receive this alert if power fails on the ME 3400G-12CS-DC switch with two power feeds, we recommend that you connect one feed to the left DC power terminal block and the other to the right DC power terminal block. (See the example in Figure 1.)

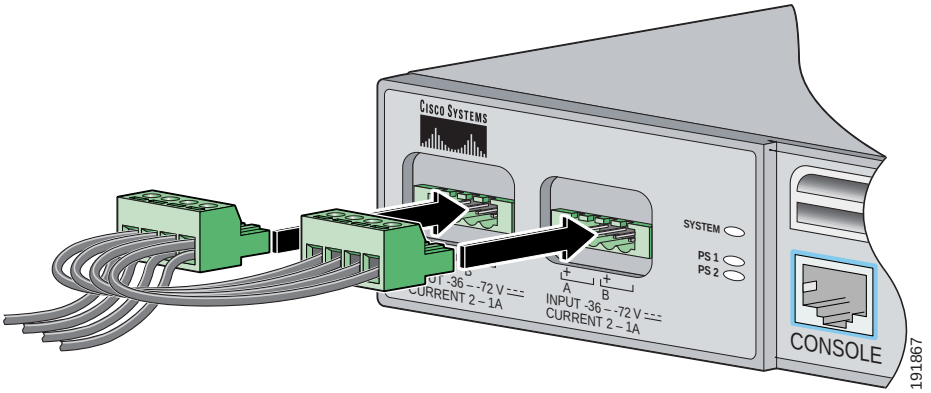
Figure 1 Connecting Separate Feeds to Each of the DC Power Terminal Blocks



1	Primary power feed	**2**	Secondary (redundant) power feed

If you want an alert if an external power supply fails, do not connect feeds to one terminal block and from there connect feeds to the second terminal block. (See the example in Figure 2.) This configuration provides redundant power, and the switch continues to operate if one of the external power supplies fails. However, the software does not send a message to you that an internal power supply has failed.

Figure 2 Connecting Feeds from One Terminal Block to the Second Terminal Block



Related Documentation

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6580/tsd_products_support_series_home.html

- *Cisco ME 3400 Ethernet Access Switch Software Configuration Guide*
- *Cisco ME 3400 Ethernet Access Switch Command Reference*
- *Cisco ME 3400 and ME 2400 Ethernet Access Switch System Message Guide*
- *Cisco ME 3400 Ethernet Access Switch Hardware Installation Guide*
- *Cisco ME 3400 and ME 2400 Ethernet Access Switches Getting Started Guide*
- *Regulatory Compliance and Safety Information for the Cisco ME 3400 and ME 2400 Ethernet Access Switches*
- *Configuration Notes for the Cisco ME 3400G-12CS Ethernet Access Switch*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Note*
- These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

  - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
  - *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
  - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
  - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2008 Cisco Systems, Inc. All rights reserved.